IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL.,	)	
	)	
Plaintiffs,	)	
	)	Civil Action No.
vs.	)	
	)	1:17-CV-2989-AT
BRAD RAFFENSPERGER, ET AL.,	)	
	)	
Defendants.	)	

VIRTUAL VIDEOTAPED 30(b)(6) DEPOSITION OF
SANFORD MERRITT BEAVER
Thursday, March 10, 2022
9:09 a.m.
VOLUME II (Pages 260 - 439)

Robin K. Ferrill, CCR-B-1936, RPR

INDEX

VIRTUAL VIDEOTAPED 30(b)(6) DEPOSITION OF SANFORD MERRITT BEAVER

Thursday, March 10, 2022

DESCRIPTION OF EXHIBITS

INDEX CONTINUED

DESCRIPTION OF EXHIBITS

INDEX CONTINUED

DESCRIPTION OF EXHIBITS

INDEX CONTINUED

DESCRIPTION OF EXHIBITS

(Original exhibits attached to the Original transcript.)

MR. TYSON: Good morning. Bryan Tyson for the State Defendants.

MR. MILLER: This is Carey Miller, also here for the State Defendants.

MR. LOWMAN: This is David Lowman for the Fulton County Defendants.

MS. GREENHALGH: Susan Greenhalgh, consultant to Coalition for Good Governance.

MS. CONNORS: This is Jill Connors, paralegal for Ichter Davis for Coalition Plaintiffs.

THE VIDEOGRAPHER: Thank you.

Would the court reporter please swear in the witness.

SANFORD MERRITT BEAVER,

called as a witness, having been duly sworn by a Notary Public, was examined and testified as follows:

EXAMINATION

BY MR. CROSS:

Q. Good morning, Mr. Beaver.

A. Morning.

(Plaintiffs' Exhibit 1, Fortalice Solutions Technical Assessment Prepared for Secretary of State Georgia, DRAFT - May 19, 2020, Bates

Q. Okay.
A. I would have to verify that.
Q. So were there any other documents you looked at beyond those 20 to prepare for today?
A. No.
Q. Was there anyone you spoke with or met with to prepare for today?
A. With counsel.
Q. Anyone other than counsel?
A. Not in specific to prepare for this.
Q. All right. Take a look at Exhibit 1, if you would, please, the May 19 Technical Assessment.
A. Okay.
Q. And turn to Page 1 under the Executive Summary, please.
A. Okay.
Q. And this provides, with the Background and Tasks, just a high-level overview. It indicates that "In April of 2020, Secretary of State Georgia contracted with Fortalice Solutions Offensive Cybersecurity Operations team to perform a penetration test from the perspective of a remote worker during COVID-19 adjustments. Fortalice conducted testing in May of 2020."
Do you see that?

A. Yes.
Q. Is that a generally accurate overview of what the purpose of this particular assessment was?
A. Yes.
Q. And then if you come under, you see Offensive Cybersecurity Assessment Approach & Results and then Remote User Assessment.
Do you see that?
A. Yes.
Q. And then below that, it reads "The goal of the remote user penetration testing scenario was to identify any issues with the configuration of technology or services that a malicious user could exploit to gain further access into, and potentially take control of, the network."
Do you see that?
A. Yes.
Q. And do I understand correctly when it refers to "remote user assessment" or "remote user penetration testing," do I understand you correctly that Fortalice was doing this remotely? They were not physically on site with whatever network they were trying to penetrate; is that right?
A. Correct. That is correct.
Q. And did they do this from their offices or

do you know where they were located when they did it?

A. No. I don't know where they are doing it from.

Q. Did it matter?

A. No, it's the Internet. You can do it from anywhere around the world.

Q. All right. Take a look at -- if you come further down the first page under Commentary, it reads "The report provides findings and action plans for those findings. However, across the components of penetration testing, six overarching trends surfaced. Fortalice recommends that Secretary of State Georgia address these themes in order to quickly protect itself should an actual breach occur."

Do you see that?

A. Yes.

Q. And then those six overarching findings are listed below in Figure 1, right?

A. Yes.

Q. And each of those in Figure 1 is identified as a Critical or High Vulnerability.

Do you see that beneath Figure 1?

A. Yes.

Q. And the first one of these is Multi-Factor

A. No.

Q. And do I understand correctly, when I was reading through this report, I didn't see anything that indicated that part of what Fortalice was doing was to determine whether any of the vulnerabilities they identified had been exploited. That was not part of the scope of this work; is that right?

A. Correct.

Q. After these vulnerabilities were identified, did the Secretary's Office task Fortalice or anyone else with that type of assessment to determine whether any of these vulnerabilities had been exploited?

A. We did not ask anybody, a third party to do anything.

Q. And no one internal at the Secretary's Office undertook that assessment, right?

A. Correct. There was no evidence that there was an exploitation, thus there was no forensics requested.

Q. Right. But there was also no effort made by the Secretary's Office to look for that evidence, right?

A. Correct. We don't look for evidence of something that we -- nobody has ever identified that

there was an issue.

Q. Okay.

All right. If you look at -- still on Page 1 of Exhibit 1, this May 2020 Technical Assessment, the next one down, the next critical finding refers to Insecure File Shares.

Do you see that?

A. Yes.

Q. And here reads "Fortalice discovered that open file shares existed on the network to which all domain users had access."

A. I --

Q. Right. Sorry.

And then it goes on. "The affected shares introduced varying degrees of information disclosure, and in at least one instance exposed the username and password of an administrative account."

Do you see that?

A. Yes.

Q. An administrative account in this context is an account that gives broad access and control to whoever has access to that account over the corresponding network; is that right?

A. Administrative access to a specific system. This system happened to be an internal web server,

which was our Intranet site. So the administrative access would be able to look at documents that our professional licensing group gives.

Q. An administrative account would also have the ability to add, delete, alter documents in that environment, right?

A. For professional licensing.

Q. And when you say "professional licensing," what does that mean?

A. We, Secretary of State, is in charge of four agencies: Elections, Corporations Registration, Professional Licensing and Securities. Professional Licensing handles 40 boards, including nursing, electrical -- electricians, landscaping, a number of different -- cosmetology.

Q. Was there anything else on this Intranet regarding the insecure file shares beyond professional licensing materials?

A. That was the area that this specifically targeted.

Q. Turn to Page 11, if you would, please. Just let me know when you have that.

MR. DENTON: David, to confirm, this is the numbered Page 11, not Page 11 of the PDF?

MR. CROSS: This is the page at the bottom

it's exposed to the outside.

We have many layers. And some layers, some vulnerabilities we can't fix. So you put over things on top of it to protect. And as it said in our red hat, we haven't had enough layers to protect somebody from getting into our system.

So this is an internal website. So somebody would have had to breach into the system first to be able to navigate to this. The red hat test did show that we had sufficient layers of security to keep people out.

So yes, we are addressing it, but it's a two-year effort to fix this problem.

Q. Okay.

A. We are in the process now of going to a new system.

Q. Take a look at Page 2, if you would, in that Figure 1. At the top it reads Administrative Password Reuse.

A. Yes.

Q. And here Fortalice reports that it observed a -- "Fortalice observed a solution in place to prevent administrative password reuse at Secretary of State Georgia, but the implementation seems incomplete. Until this task is finished, the risk

remains for attackers to reuse administrative credentials across some machines."

Do you see that?

A. Yes.

Q. What's the risk associated with users reusing administrative credentials?

A. What is the risk?

Q. Yes. Why is reuse of administrative credentials considered a security risk?

A. Well, this specific thing was speaking to the administrative password used to set up a laptop. So what they are speaking is that reusing administrative passwords, if you have -- somebody discovers that administrative password that you can potentially get on to a laptop.

Q. Right. But why is reusing that password a security risk? Meaning having multiple administrative accounts having the same password, why is that a problem?

A. Well, again, if somebody was to discover that password, they could get into the system -- into a laptop. So reuse -- security has different, I'll say, levels. You can put such security on a system that you can't use it because it's so secure. It could have no security and everybody can use it, but

then it's open.

So this is -- remember, I said earlier, these are cut and paste for these kinds of things. Setting up laptops, everyone having its own unique administrative password, although it would be very, very, very secure, would become then a problematic to actually being able to maintain your laptop across the business.

So it's a risk balance. You can -- if you -- somebody has a problem with their computer and every single laptop has its own administrative password, you now go out to try to fix it and the person trying to fix it wouldn't necessarily be able to get on to that machine if they didn't know the unique password that was set up for administrative password.

Fortalice is telling us here, there is -- you know, by reusing it you have an exposure. But I can tell you from my prior experience and talking to other organizations, this is what every organization I know does is they set up an administrative password for a setup setting up laptops. Yes, there is a potential risk. There's risk with everything. This is a measured risk. Organizations have gone this direction because of support issues. In order to

support your laptops, they use the same administrative password on all of them.

That is not unique to Secretary of State. That is pretty much an industry -- the way the industry is. And you could probably query numerous businesses and ask do they use the same administrative password for setting up every laptop, probably the answer is yes. Is that a risk? Yes. It's a measured risk.

Q. But the administrative password that's used in that context to set up a laptop, that's a password that's specific to a particular administrative account, correct?

A. For setting up laptops. It's specifically for setting up laptops. Not to be used anywhere else.

Q. Right. But it's not a password that's specific to a particular laptop. It's a password that's used for an administrative account that whoever is responsible for that account or has access to that account can then use that access to set up any number of laptops; is that right?

A. Correct.

Q. Okay. And it is commonly understood in cybersecurity that the more a particular password is

reused across accounts, the greater risk that it is disclosed or it's leaked in some way, right?

MR. DENTON: Object to form.

You can answer, Merritt.

A. Okay. So the answer to that is yes. But that's not what that -- this is talking about here. This is not talking about using the same administrative password for setting up laptops as for accessing servers. This is strictly the password for setting up laptops.

Q. (By Mr. Cross) And then if you come to the last vulnerability in Figure 1, here it reads "Fortalice discovered a domain administrator username and password in cleartext. If the machine housing this file was compromised, it could result in the immediate compromise of the entire domain."

Do you see that?

A. Yes.

Q. What is cleartext?

A. Unencrypted. So that means the password was stored unencrypted. And the system it's talking about here, the domain it's talking about here is our BOSS Ticketing System. So if somebody was to compromise it, the domain would be our Ticketing Environment. So somebody could come in, if they were

able to figure out how to get into this system, see all tickets that were submitted.

Q. Sorry. What was the first -- did you say BOSS Ticketing System?

A. Yes. BOSS is the company, Business Automation System, something like that.

Q. How do you spell that?

A. So the ticketing system is -- B-o-s-s.

Q. Oh, okay. Just like the word. And -- sorry, what you were going to say, what's the ticketing system?

A. Ticketing is how users, SOS users internally can submit a help desk ticket for support.

Q. And when you say help desk, you mean IT?

A. Yes. Yes.

Q. And what, if anything, was done to address the cleartext password disclosure vulnerability there?

A. I don't know. I did not hear what -- that was done. It's a fairly low-risk system, so it's probably on a -- I can only guess.

Q. And I'm not asking you to guess. Do you know whether steps were actually taken or you don't know one way or another?

A. I don't know one way or another.

Q. Coming back up to the administrative password reuse vulnerability we just looked at, do you know what, if any, steps were taken to remedy that?

A. No, I don't.

Q. Okay. If you wanted to know the answer to that question who would you ask?

A. Well, the person's -- it would probably be either Jason Matthews or Bill Warwick, but they don't work here anymore. But they were here at the time, back in 2020. They might know whether or not that was changed.

Q. Anyone who currently works at the Secretary's Office or Fortalice you think would know the answer?

A. I doubt it. If they changed it, it would have just been part of our regular routine password maintenance. And so whether or not it was changed as part of this or changed as part of our regular process, the existing people probably wouldn't know the distinction.

Q. All right.

Turn to Page 5, please. And we are still looking at this May 19, 2020 Technical Assessment.

Do you see the heading 2.1 Remote VPN User

assessment we were just talking about?

A. A prior assessment, yes. That we talked about before, yes.

Q. And -- sorry. But when you say that they did a prior assessment of the balloting system and the voting machines, were those part of the same specific assessment? They were not separate assessments for Fortalice; is that right?

A. Yes, there was only one.

Q. The election results are communicated to the State from the counties through the election night reporting system, right?

A. Yes.

Q. And those are communicated via the Internet, right?

A. Yes.

Q. Why not have Fortalice do a security assessment of that system given it's Internet connected?

A. That is a cloud service that we buy from a third party vendor. So it's not in our network domain.

Q. Who is the cloud service provider for that?

A. I think it's Scytl, S-c-y-t-l. May be an "E" on the end.

Q. So you rely on the Scytl for the security of that system; is that right?

A. Yes.

Q. And do you require Scytl to conduct annual cybersecurity assessments of the ENR system?

A. We, as part of our contract, give them a security requirements document that they sign off that they have completed and maintain.

Q. But that's a document they send back to you, what, each year?

A. I don't see a document from them each year. I do get a report from -- I will say from time to time I have seen a report that they have submitted. But I wouldn't say that I get an annual report.

Q. How often does that report come in?

A. As I said, I don't recall.

Q. Do you recall at any point any of those reports identifying any election -- or, I'm sorry, strike that.

Do you recall any of those reports at any point identifying any security vulnerabilities or concerns of any kind?

A. No.

Q. But that's not something you reviewed for today; is that right?

Office would you expect those reports to be maintained, if at all?

A. I don't have a specific place that I would know to go look.

Q. What are the specific security requirements the State has for Scytl?

A. There's a document that we give all vendors. It's part of our contracting process.

Q. Do you know what the security requirements are in that document?

A. I would have to go review it. And over time that document changes as more security things are identified. So back when it was given to them, I don't know -- I couldn't tell you what the document looked like compared to the one that we use now.

MR. CROSS: All right. Take a look at Exhibit 2, if you would, please.

(Plaintiffs' Exhibit 2, Fortalice Solutions Firmware Comparison and Configuration Analysis, Secretary of State Georgia, DRAFT - July 9, 2020, Bates labeled FORTALICE003807 - FORTALICE003811, marked for identification.)

Q. (By Mr. Cross) Just let me know when you have it, sir.

A. I have got it.

Q. Do you see that this is entitled Fortalice Solutions Firmware Comparison and Configuration Analysis Secretary of State Georgia, Draft - July 9, 2020?

Do you see that?

A. Yes.

Q. Is this a document you recall seeing before?

A. No.

Q. Do you remember having any involvement with Fortalice when they prepared -- or did the underlying analysis for this report?

A. No.

Was this one of the 20 documents you sent?

Q. I didn't send any documents, so I'm not sure what you mean. We got documents from Fortalice, and this is -- if you look at the bottom, you can see this is one of the documents they produced to us.

A. So I have not seen this document before.

Q. Sorry. And one quick question for you. The Exhibit 1 that we looked at, that Technical Assessment, also the one here in Exhibit 2, we went through the State's production and we couldn't find copies of these or versions of these. Do you know why the State would not have these documents itself?

Why only Fortalice would have them?

MR. DENTON: Object to the form.

A. Fortalice -- Fortalice did not send them to us.

Q. (By Mr. Cross) Oh, I'm sorry. Why is that?

A. We chose to just review outcomes in a conference call.

Q. Oh, is this -- okay. So is this what you talked about earlier in a prior deposition that beginning sometime in 2019, you instructed Fortalice not to put stuff in writing? That you guys now rely on, I think you said, oral meetings?

A. Yes.

MR. DENTON: Object to form.

Q. (By Mr. Cross) All right. Take a look at Exhibit 2, if you would, please, and look at the top of Page 2.

Again, I'm using the pagination numbers on the document. And at the top it says Assessment Report, Background and Tasks.

Do you see that?

A. Yes.

Q. Here writes "In May of 2020, as part of an ongoing relationship with Secretary of State Georgia, Fortalice Solutions conducted a system review of

network assets and critical systems. The Fortalice team performed testing and reviews during the months of May and June 2020. The objectives of these tasks were to identify weaknesses in the configuration of equipment on Secretary of State Georgia's networks and produce the following documents."

And then below, you see there's two documents indicated there. The first is a "configuration review report," the second is a "set of recommendation workbooks."

Do you see that?

A. Yes.

Q. Do you recall receiving those reports or documents?

A. No.

Q. Would you have expected to or would you have expected them just to hold on to those internally and communicate them orally?

A. Orally.

Q. If you come to the next paragraph, here Fortalice wrote "Securely configuring assets is an important part of defense in depth and can limit the extent of a compromise in the event a vulnerability is exploited. Adhering to an industry-recognized benchmark avoids the need to create one and makes it

easier to measure adherence during internal tracking and when proving security posture to an auditor."

Do you see that?

A. Yes.

Q. Do you agree with that?

A. I think it's an okay statement, yes. It is an ideal situation.

Q. Why is it important to adhere to an industry-recognized benchmark for cybersecurity?

A. When going through the process of setting up cybersecurity, if you use industry standard processes, it's easier to go through one to validate what your security levels look like, and it's easier to identify, you know, areas that you might be missing or need to work on.

Q. And how do you determine what an industry-recognized benchmark is in the cybersecurity context?

A. Well, for example, NIST is a standard -- industry-standard organization. And they do a number of industry-standard security measures to help you -- basically help guide you on what levels of security and what layer -- you know, security is a variable thing.

Take passwords is a good example of

security. As an individual organization, if you try to determine by yourself what level of password strength should be, you may or may not be doing something that's sufficient or you may be overly sufficient. NIST has identified that 16 characters of any kind is sufficient, that it would take a lifetime to break.

Now, if we went out on our own, we might say "Oh, let's do 64 characters." Well, that would be really strong, but we would put an undue burden on our users to try to remember a 64-character password, when NIST helps us understand that, for right now, password length, 16 characters of any character is sufficient.

So that's why they are saying here using an industry-recognized benchmark so that we don't have to do all of the analysis ourselves.

Q. When Fortalice indicates here that "Adhering to an industry-recognized benchmark makes it easier to measure adherence when proving security posture to an auditor," what does that mean, "proving security posture to an auditor"?

A. Let's use the same example I used before. Password. If an auditor comes in and we are saying "Well, we are using eight characters but they must

have this structure" versus the auditor says "Well, I'm using NIST, who says you should have 16 characters of any structure," it makes it easier if we follow an industry standard process for us defining how we set passwords.

So the auditor isn't left to go figure out "Okay. If I've got eight characters what they can use, capitals, lower-cased, numbers, symbols," is that equivalent to using 16 characters that are all, let's say, lower case? Somebody then has to go do research to determine what are the possibilities with eight -- with all these variables versus 16 with those lower set of variables. It just takes work.

So for an auditor to understand, following an industry's recognized benchmark makes it simpler to assess is what we're saying.

Does that answer your question?

Q. It does, yes. Thank you. It's very helpful.

Does "auditor" in that context, does that include, like, the red team audit that Fortalice does here?

A. We did not have audits done. We had assessments done.

Q. That's what I want to understand. So, in

We have had to come up with our own way of managing those passwords that won't tie into our central management system. Every business is like that. We are not unique.

Q. You agree that strong authentication mechanisms are important, though, right?

A. I would say yes.

Q. Why is that important?

A. Authentication is an example as we used before with NIST. They define -- help us define what a good, strong password would be. If you -- the weaker the password, the better -- the more likely that password could be breached or guessed.

Q. Right.

Turn to the next page if you would. At the top it says Logging Policies.

A. Yes.

Q. And here reads "Current logging configurations could cause difficulty if an incident occurred. In order to collect useful logs, devices should log all messages except debug level messages, and offload these messages to a remote logging server."

Do you see that?

A. Yes.

Q. Okay. And just so I understand, you are not aware of any investigation done by anyone at the Secretary's Office to determine whether what's listed here as a finding by Fortalice, whether there were, in fact, devices that had FTP and HTTP enabled; is that right?

A. That is correct. And that probably would have been brought up. I know in prior years, back in the probably 2015 timeframe, we ran into a number of HTTP web services and file transfer protocol folders on servers that we had to fix. And it was rather vocal conversations going on back and forth on doing that.

So I think the team knew that that was something that if we found that going on, I probably would have heard about it.

Q. Do you agree that a commonly accepted cybersecurity practice is to disable unnecessary services on devices?

A. Yes.

Q. And why is that?

A. If you are not using basically a port or a feature, don't leave it on. Because it potentially, potentially could eventually become a vulnerability.

Q. And then if you look in this -- the next

sentence after we just read, it goes on to say "These services should be reviewed to ensure that any non-essential services are disabled in order to reduce Secretary of State Georgia's attack surface."

Do you see that?

A. Yes.

Q. Why is it important, as a general matter, to reduce the Secretary's attack surface?

A. Part of security is to eliminate the vectors of attack.

Q. And vectors, you mean -- sorry. Just in sort of nontechnical speak, sort of the vulnerabilities that you guys have, Fortalice and others, assessed. Is that what you mean? Because "vector" is another word for vulnerability.

A. Basically, if you eliminate the number of points a potential attacker could attack.

Q. Sorry. Just in layman terms, when you say vectors is a technical term, do you mean vulnerabilities?

MR. DENTON: Object to form.

A. Vulnerability would be one, a vector.

Q. (By Mr. Cross) All right. And then if you come further down the page, do you see security Updates?

A. Yes.

Q. And here it reads "Based on the current configurations, the Palo Alto firewalls are potentially set to not automatically install updates."

Do you see that?

A. Yes.

Q. As a general matter, why is it important to use up-to-date software for cybersecurity purposes?

MR. DENTON: Object to form.

A. There's numerous reasons to update and other reasons to not update. So updating isn't always the best path.

Q. (By Mr. Cross) Can you tell me --

A. So -- so updates, many times a manufacturer will find a vulnerability or a feature enhancement in part of their patches. A vulnerability is something that somebody has identified -- and it may be themselves, it may be a third party company who is paid to go look for stuff or it could be a hacker -- has identified a vulnerability. And a company will go in and basically fix the problem so that vulnerability goes away.

Enhancements are things or features such that somebody -- a company would do to enhance their

product or make their product better. Doing automatic updates is a risk. Because until you assess whether that update will adversely impact your security environment, you may be introducing new problems.

So on one hand, you could say that automatically doing updates is good if you just have no ability to go look at those patches to see whether or not they are going to affect you adversely. So it's a measured risk.

Q. As a general matter, is it accepted practice, accepted cybersecurity practice to implement updates that are offered to patch vulnerabilities in a system? As opposed to what I think you referred to as, like, a feature enhancement?

MR. DENTON: Object to form.

A. There are different types of updates. There are different types of updates. Some are more automated, such as blacklisted IP addresses. Those, typically, you automate those. But patches for vulnerabilities, that -- that has to be assessed in your specific environment, whether or not you really want to do that or not.

Q. (By Mr. Cross) Under what circumstances

would you envision not accepting a patch for a vulnerability in the software?

A. Well, patches don't necessarily come in saying "This is for a vulnerability." It just says "patch."

Q. So you may not know that a patch coming in includes a vulnerability patch. Is that the idea?

A. Not until you research it.

Q. If you look back at Page 3 under Results, very bottom of the page, do you see the second sentence reads "The workbooks included alongside this report will allow Secretary of State Georgia to review any configuration in question to increase the security of the organization's baseline."

Do you see that?

A. Yes.

Q. And do I understand correctly that there would not have been workbooks provided in writing because of the directive you talked about earlier given to Fortalice?

A. Correct. So once again, this kind of shows you that this was probably a cut and paste.

Q. And as you sit here today, I may know the answer to this because you said you weren't familiar with the report, but just to be sure, as you sit

here, are you aware of any efforts undertaken by anyone in the Secretary's Office to address any of the findings in this report?

A. No.

Q. All right. Let me grab the next exhibit. And if you want to take a break at any point, Mr. Beaver, just say the word.

MR. CROSS: Okay. This is going to be Exhibit 3.

All right. You should be able to grab Exhibit 3 now.

(Plaintiffs' Exhibit 3, Fortalice Solutions Technical Assessment Prepared for Secretary of State Georgia, DRAFT - August 25, 2020, Bates labeled FORTALICE003692 - FORTALICE003704, marked for identification.)

A. Okay. Technical Assessment.

Q. (By Mr. Cross) Yes. And so this one is labeled Fortalice Solutions Technical Assessment Prepared for Secretary of State Georgia and it's dated August 25th of 2020.

Do you see that?

A. Yes.

Q. And if you look on this -- by the way, you will see on the cover page and at the bottom, there's

Q. Do you see the second paragraph, the first full paragraph begins "The overall theme"?

A. Yes.

Q. And here Fortalice wrote "The overall theme Fortalice discovered throughout the test was a lack of secure coding principles."

Do you see that?

A. Yes.

Q. And why is it important to adhere to secure coding principles when doing coding? Like, creating software?

MR. DENTON: Object to form.

A. Secure coding principles -- without following good, secure coding principles, you leave code open to attacks, such as SQL injection and cross-site scripting. Those are two common examples.

So it looks like they were looking at the code, and it identified the code had potential weaknesses. Now, because we know the code has potential weaknesses, we use a layer on top of this that blocks those kinds of attacks. We have a system that we route all requests through, which basically scour the web requests and look for any types of non-basically direct use of the system, where somebody is trying to inject code because we know

that these -- the code has these issues.

So this is -- what we talked about earlier of you putting layers of security to protect any known vulnerabilities.

Q. (By Mr. Cross) And the layer you are talking about now, that would protect against SQL injection, right?

A. Yes.

Q. And just so we are clear, SQL injection -- I guess maybe it's easier to put it this way. SQL injection can occur when a user goes to, like, a website, for example, where they can do a search. And instead of conducting a legitimate search, they put in various terms that causes the system to return information that it shouldn't if it has a vulnerability that allows that. Is that generally right?

A. That's -- that's pretty close.

Q. Right.

A. So our system looks at if you are trying to put in a date field for birth date and you put something else in there, it blocks it. If you have your name, put your name here, and you put in something, a SQL call, it blocks it. And there aren't too many SQL calls that start with Merritt

Q. And the situation you are talking about is one I think we talked about in the prior deposition that went back -- that came to light shortly before the 2018 election, right?

A. Yes. Yes.

Q. And so that anticipates the question I was going to ask you. Given whatever measures were taken to address that situation in 2018, do you have any insight as to why Fortalice found the vulnerability found here with the absentee ballot system almost two years later in August of 2020, or do you just not know one way or the other?

A. As I stated earlier, a lot of the stuff is in the code, can't be changed. So even though we had identified it, we had put some defense -- or basically defenses, some layers of security to keep the problem from being -- getting worse or doing what they are saying.

But the code in itself was -- still had the weakness in it. So if you can't change the code, you put layers of security around it to reduce the risk. What they have done here is they have reidentified the same problem that we knew we had. But we have put other defenses to basically support this.

So it doesn't get rid of the problem. It's

known. It's existing. We just now mitigated the issue in a different way.

Q. All right. Let me grab the next exhibit.

MR. CROSS: This should be Exhibit 4, I believe. Yes.

(Plaintiffs' Exhibit 4, Fortalice Solutions Technical Assessment Prepared for Secretary of State Georgia, DRAFT - August 25, 2020, Bates labeled FORTALICE003625 - FORTALICE 003639, marked for identification.)

Q. (By Mr. Cross) You should be able to pull that up now, Mr. Beaver.

A. Okay. Is this the same one? This is Technical Assessment. Was the last one a Technical Assessment?

Q. Yes, but they are -- hold on. Let me look real quick.

They were prepared the same day but are different reports. You can confirm this for yourself. There are going to be three documents for you to look at. They are all Technical Assessments dated August 25, 2020. It looks to me like there were three different reports that were drafted looking at three different things as part of this assessment. We'll kind of walk through them now if

that's wrong.

So this is another August 25th, 2020 draft Technical Assessment from the Secretary's Office.

Do you see that?

A. Yes.

Q. And if you come to Page 2, this gives the overview for this report. And here you can see it's -- it's similar to the overview for the last one, but here it talks about performing a web application assessment against the My Voter Page site.

Do you see that?

A. Yes.

Q. And so --

A. Which I think the last one was an assessment of the My Voter Page also.

Q. Well, I guess that's what I'm going to raise with you, because as I read these, that's not right. So if you need to go back to Exhibit 3 and grab that, Exhibit 3 refers to the ballot request and ElectioNet sites, which are distinct from the My Voter Page site, correct?

A. I think you can get -- your ballot request is on -- is a tab on the My Voter Page.

Q. Okay. So is it your -- are you guessing

to. I can't be positive, but that makes sense. Because that was when Fortalice got involved to look at this and when we put measures in place to block it.

And as I said, the code's still there. We just have security measures that block that kind of activity since we can't change the code.

Q. All right.

MR. CROSS: Let me -- you should be able to pull up Exhibit 5 now, which is -- you'll see it's the third assessment I mentioned before. It's the same date.

(Plaintiffs' Exhibit 5, Fortalice Solutions Technical Assessment Prepared for Secretary of State Georgia, DRAFT - August 25, 2020, Bates labeled FORTALICE003678 - FORTALICE003691, marked for identification.)

Q. (By Mr. Cross) Just let me know when you have that.

A. I've got it.

Q. And if you come to Page 2 of this Technical Assessment, also dated August 25th, 2020, you see where the Executive Summary is?

A. Yes.

Q. And here, the Executive Summary is similar

to the prior two August 25th, 2020 overviews except you see here this one is an assessment of the Online Voter Registration site?

A. Yes. It looks like they are changing the text between different documents of the same thing. So your Online Voter Registration site is your MVP page. So my -- and if you notice, we are still talking about cross-site scripting. So it's -- to me, it looks like it's just different versions of the same document from his same assessment, but the person is updating it with more current information. And since it says Draft, you are probably looking at different versions of when -- you know, when he has updated to get more -- from his cut and paste -- to get more accurate information.

That -- but I didn't build this document, so I can only speculate. But from what it looks like, it looks like the same assessment, just different versions of the document.

Q. So you have not seen this report before either; is that right?

A. Correct. I can only speculate.

Q. I will not ask you to do that.

I do have a question, though. If you turn to Page 8 -- and you can look at Page 7 and 8

that came out of this report or just other types of security things we do on a general basis.

Q. So again, this report is dated July 1 of last year. Are there any specific security measures that you are aware of that the Secretary's Office implemented since July of 2021, last year, to protect against vulnerabilities with the voting equipment?

MR. DENTON: Object to form.

A. I am not aware of it.

Q. (By Mr. Cross) Sorry. You said you are not aware?

A. I am not aware, but that doesn't mean none happened. I'm just not aware. Understand, counties manage the equipment, not the Secretary of State's Office.

Q. And are you aware of any measures taken by any county of Georgia since July of 2021 to address vulnerabilities with the voting equipment?

MR. DENTON: Object to form.

A. I'm not aware.

Q. (By Mr. Cross) Are you aware of any measures taken by the Secretary's Office to address vulnerabilities with the voting system more broadly since July of 2021?

MR. DENTON: Object to form.

A. That's a broad question. Voting system is a lot of different pieces and parts. Which one -- what are you specifically asking about?

Q. (By Mr. Cross) So one of the responses the State has made in response to this July 1 report from Dr. Halderman is that, you know, some of the vulnerabilities he finds, like, for example, the ability to upload malware through a USB port on the voting equipment, are you aware of any measures taken by the Secretary's Office or by a county to increase security around access to those ports or to the machines?

A. I'm not aware. That doesn't mean it hasn't been done.

Q. Are you aware of any measures taken by Dominion to address vulnerabilities with their own voting equipment since July of 2021?

A. I'm not aware.

Q. Do you know whether anyone at the Secretary's Office has discussed Dr. Halderman's report with anyone at Dominion? This report?

A. I'm not aware.

Q. If you wanted to know the answer to that, who would you ask?

A. I might start with Gabe Sterling or Michael

should be public? Publicly released?

A. I don't think that's my decision.

Q. Okay. But you are the Chief Information Officer for the Secretary's Office. Do you have a view from a cybersecurity perspective on whether this report, which purports to identify numerous vulnerabilities with the voting system, whether it should be released publicly?

A. Anything that can adversely effect security, in my opinion, shouldn't be released. You are only reducing Georgia's ability to secure their equipment and systems whenever security information about an existing system is released. In my mind, it's bad practice and just, you know, being ignorant of cybersecurity.

Q. Last couple questions or couple points.

What are the industry-recognized benchmarks that the Secretary's Office attempts to adhere to for cybersecurity for the voting system, if any?

MR. DENTON: Object to form.

A. That is way too broad of a question.

MR. CROSS: Fair enough. Let me narrow it down. Let's just focus on the Dominion equipment, the BMDs, the printers, the scanners.

Q. (By Mr. Cross) What, if any,

industry-recognized benchmarks does the Secretary's Office try to adhere to for securing that equipment?

A. Once again, you are -- it's a very broad question. You would have to be very specific. Everything from physical to software to wireless and hard networks, there's a whole range of attack vectors to take into consideration. We use that word. It's a common term in cybersecurity.

So when you say what avenues, I mean, someone could talk for days on the attack vectors that one should look at. So I can't be specific with it, that broad of a question.

Q. And why should one look at the attack vectors of that equipment?

A. Basically attack vectors are where systems can be compromised. And so reducing attack vectors is always your first defense. And then once you have vectors that you can't get rid of, then what do you do on those vectors?

Q. If I wanted to understand -- or strike that.

If I wanted to understand what the industry-recognized benchmarks are that the Secretary's Office attempts to adhere to with the voting equipment that we -- just the Dominion

MR. DENTON: Yes, I saw the application. I just haven't seen anything further.

Thank you.

MR. HAVIAN: You are welcome.

(Plaintiffs' Exhibit 11, Curling Plaintiffs' Fifth Amended Notice of Deposition of Office of the Secretary of State, marked for identification.)

Q. (By Mr. Havian) Okay. Mr. Beaver, let's jump right in. I would like to have you take a look at Exhibit 11.

A. Okay.

Q. Which is a Notice of Deposition. And the pages, at least on my copy, do not appear to be numbered. But if you could -- if you could scroll down to Topic Number 10, which is about three-quarters of the end of the document.

A. Does it start with any instance in 2020 and 2021?

Q. Correct. That says "Any instance in 2020 or 2021, within the knowledge of the Secretary of State's Office, when a person or entity other than an authorized election worker or Georgia state or county official obtained voting data from a Georgia election or images of voting equipment used in a Georgia

election."

Do you see that?

A. Yes.

Q. That's going to be the primary area of my focus today. Are you prepared to address that issue today?

A. I can answer to my knowledge.

Q. Have you taken any steps to gather knowledge of any other persons in the Georgia Secretary of State's Office about this issue?

A. No.

Q. Okay. I believe it was yesterday or perhaps the evening before yesterday, Mr. Bruce Brown, counsel for the Coalition, sent an e-mail to Mr. Russo and Mr. Miller asking that you, in particular, focus on a particular aspect of Issue Number 10. And I'll read that to you. It says "That examination will focus primarily on the events discussed in the audio recording marked as Exhibit 12 and played at the deposition of Gabriel Sterling involving the imaging of election hardware and software in Coffee County. Please ensure that the witness is prepared to address that aspect as well as the other aspects of Issue 10."

I guess my question is, are you aware --

me.

So the fact that I didn't hear anything from him, I know his answer. I might talk to Gabe Sterling. I might talk to Michael Barnes. Those would be my starting points.

Q. And who is the security person that you are referring to?

A. Kevin Fisk.

Q. All right. So let me ask you a few other questions, more general questions about Coffee County.

First of all, are you aware that Mr. Gabriel Sterling gave a deposition in this matter as well?

A. I just heard about it. I have no details on it.

Q. I'm going to read to you something that Mr. Sterling said in his deposition and ask you whether you agree with his statement or not.

Mr. Sterling testified, quote, "Physical security is the -- obviously, the frontline of all cybersecurity. And that's one of our main things we have to worry about at all times. That's why we -- we work with the counties to make sure they have these things in under lock and key," close quote.

Do you understand the sentence I just read to you about physical security?

A. Yes, I do.

Q. Do you agree with Mr. Sterling's testimony?

A. I do.

Q. Can you explain why physical security is so important in election security?

A. Physical security is one vector of attack for someone who is trying to do some malicious damage to the environment. So protecting physical access is one avenue that you have to go after to make sure that the system is secure.

Q. To your knowledge, has the Secretary of State taken any steps since the 2020 Presidential election to investigate the physical security of the election hardware and software in Coffee County?

A. In Coffee County? I -- specifically, that county, I can't speak to. I know that we do a number of things to monitor all counties, so Coffee would be included in that.

So -- but I don't know of anything specifically targeting Coffee County. Coffee would be included in the -- in the monitoring for physical security that is done across all counties.

Q. Okay. Do you know -- can you describe for

us the activities taken across all counties to investigate the physical security of the hardware and software in the election system?

MR. DENTON: Object to form.

A. Yes. I don't have the specific requirements for each county. Each of them are required to store all the equipment in a secure location that is locked and monitored. Monitor is either -- you know, includes video and surveillance, like, Security checking on it on a regular basis.

But I don't have any specific document that I can point to that says here's what all the counties do. That -- you would have to talk to somebody in the Elections Department and -- to see what are some of the common things that are identified for counties to do. That's not my role.

Q. (By Mr. Havian) Would the copying or imaging of data, election data or election software or hardware, would that be a violation of the physical security requirements if done by anyone other than an authorized election worker?

MR. DENTON: Object to form.

You can answer if you understood the question, Merritt.

A. I think the question is obvious that yes,

that would be a breach of security, although I have yet to hear of any breach, although we do get many people who claim to do breaches that have never been proved. I would suspect that if there is such a claim right now, until someone can actually prove that that was done, that it would be in question as to the actual reality of that actually happening.

Q. (By Mr. Havian) So --

A. Has anybody tested that?

Q. Well, I'm not allowed to answer questions you ask me, although sometimes I would really enjoy doing that, but that violates the rule. So I'm afraid I'll have to leave you in suspense on that question.

I take it from your answer, is it fair to say that imaging election software or other election data is a serious, serious breach of security --

MR. DENTON: Object to form.

Q. (By Mr. Havian) -- if it happened?

A. It is a breach of security.

Q. Do you consider it a very serious breach of security if it, in fact, occurred?

A. Breach of security is serious. It's not something I would ever want to happen.

Q. Okay. And I take it from your testimony

A. Never heard that name before.

MR. DENTON: Object to form.

Q. (By Mr. Havian) The events described on this audio recording, if those events really occurred, would they constitute a violation of Georgia election rules as you understand them?

MR. DENTON: Object to form.

A. Yes. But his comments kind of lead me to believe that he's not very technical and really doesn't know what he's talking about. So I would be highly suspect of anything he's saying.

Q. (By Mr. Havian) Did you understand him to be saying that he did something technical himself as opposed to observing others doing technical things?

A. He was observing others doing technical things and was not able to very accurately reflect what potentially could have happened.

Q. Can you explain further what you mean by that?

A. Poll pads don't have a hard drive. Yet he said they imaged the hard drive on a poll pad. I would guess he doesn't know what he's talking about.

Q. Can --

A. So that kind of puts the whole conversation in question as to really did he know what he was

seeing going on.

So I would definitely would want somebody who actually understood technology and understood what was potentially going on there to do before I jumped to any conclusions. Sounded like somebody was trying to brag and get somebody's attention.

Q. So I -- you're at somewhat of a disadvantage because I have an informal writeup of what he said on the audiotape. And I apologize we didn't have a transcript for you. But I don't recall him saying that the poll pad was imaged.

A. He said he imaged everything.

MR. DENTON: Merritt, let Mr. Havian finish his question before you start to answer.

Q. (By Mr. Havian) My question is, did you hear him specifically say that he imaged the poll pad?

MR. DENTON: Object to form.

A. I heard him say he imaged everything.

Q. (By Mr. Havian) Okay.

A. And then he referenced poll pads.

Q. If it turns out that you misheard and he didn't say he -- that they imaged the poll pad or didn't mean that, would that affect your view about whether he was a suspect person providing this

information?

A. Just the whole conversation sounded suspect to me. I would want -- I would want somebody technically competent to go assess before I jump to any conclusions.

Q. Okay.

A. I have seen too many people brag that they could do something in this job only to find out they weren't even close to doing what they said they were doing.

Q. Okay.

Getting back to the specifics of the conversation, aside from the comment about imaging the poll pad, was there anything else that he said in the conversation that struck you as not plausible?

A. I would have to listen to it a few times. But the fact that he even said that he was -- that somebody in the department gave them access to image the equipment, first would be who would have done that? I would ask to go back to Coffee County and talk to the elections people there and say "Did you actually do this" or "Is this guy" -- so until you can tell me that you have got corroborating evidence from somebody else there, I would hold this whole conversation in suspect.

Q. Yes. And I take it from your demeanor it's fair to say this is such an absurdly grotesque invasion of security that it's hard for you to imagine it actually happened; is that fair?

A. Yes.

MR. DENTON: Object to the form.

Q. (By Mr. Havian) During Mr. Sterling's deposition, he testified that events in Coffee County were investigated in connection with the Presidential election of 2020.

Are you aware of any such investigation?

A. No.

Q. You are not aware of any investigation of events during the Presidential election of 2020 that occurred in Coffee County at all; is that right?

MR. DENTON: Object to form.

A. Correct. I am not aware.

Q. (By Mr. Havian) So I don't want to beat a dead horse. To the extent that Mr. Sterling testified that there was an investigation, you are just not familiar with what he's alluding, referring to; is that right?

A. Correct. If there was an investigation with a issue, it most likely would have come to me. But if it was an investigation where it was found

Q. (By Mr. Havian) Okay.

Again, focusing on Coffee County, do you recall ever hearing anything about a password being shared improperly in Coffee County, a password to the EMS system?

A. I have heard no security questions that came out of Coffee County about any topic.

Q. Were you aware that in Coffee County, as in other counties, they did a machine recount following the 2020 Presidential election?

A. Not particularly. I think there was recounts in numerous counties, and I didn't -- I don't get involved with the actual voter tabulation process. I focus on the systems at the state level.

Q. So were you aware that in Coffee County, the machinery count produced a discrepancy?

A. Okay. I'll restate. I know nothing specific about Coffee County election-wise.

Q. Do you recall hearing about machine recount discrepancies in any counties in Georgia in connection with the 2020 Presidential election?

A. I recall hearing accusations. I never heard of any actual proven issues.

Q. Okay. Do you recall anything more specific about the accusations you heard?

A. No. It was quite a while back.

Q. I'm going to ask you to take a look at the next exhibit, which will be Exhibit 13.

MR. HAVIAN: Joe, can you upload the November 2020 memo, please?

(Plaintiffs' Exhibit 13, Official Election Bulletin, dated November 17, 2020, from Chris Harvey, Elections Division Director, to County Election Officials and County Registrars, RE: Open Records Requests - Security Information Exempt, marked for identification.)

Q. (By Mr. Havian) And while we are doing that, do you recall any information about Coffee County declining to certify their results after a machine recount?

A. As I stated before, I have no knowledge of anything that was tied to Coffee County. Prior to this conversation, I can't tell you I have ever even heard anything about Coffee County as the county.

Q. Okay. Can you please pull up Exhibit 13?

A. Election Bulletin, November 17?

Q. Correct. And you may need to enlarge it on your screen in order to read it.

A. Yes.

Q. Let me know when you've got it to the point

where it's legible. Sorry about that.

A. I can see it.

Q. Okay. So first of all, take a look at this memo, which is from Chris Harvey, Elections Division Director, to County Election Officials and County Registrars, dated November 17th, 2020. And I would like to ask you if you recognize this memo.

A. No.

Q. You don't believe you have seen it before?

A. I know I haven't seen it before.

Q. I would like to ask you a few questions to see if some of these things are familiar to you, even though I appreciate you haven't read the memo before.

First of all, do you know Mr. Harvey?

A. Yes.

Q. And who is he?

A. He was the Director for Elections.

Q. And do you know generally what his responsibilities were as Director of Elections?

A. So he was responsible for running the state-level responsibilities for running elections. So that means managing the voter registration system, collecting anything that was tied to the voter registration system. They managed the election ballot count collection process.

Counties actually are responsible, by law, to actually run the elections and actually run the machines. So he did not manage that. But he did act as an adviser to the counties on the election law.

Q. Okay. So I would like to have you look at this memo and I would like to read a couple of short parts of it to you.

First, I want to start in the second paragraph --

A. Yes.

Q. -- where Mr. Harvey says "Several counties have also received Open Records Requests for the information contained in the log files of the KNOWiNK poll books."

Do you see that?

A. Yes.

Q. And then he's -- going down a couple of paragraphs, in the second to last paragraph, he says "Under the Open Records Act, providing copies of software, software updates, or thumb drives containing software or software updates is not subject to open records requests."

Do you see that?

A. Yes.

Q. And then later at the bottom of the first

page, there's the last couple lines -- well, actually it's a fairly long sentence there. But basically, he says he cannot give out software or databases except upon the order of a court of competent jurisdiction.

Do you see that?

A. Yep.

Q. Do you know why -- do you know of any reason why Mr. Harvey sent out a memo warning people about turning over copies of software, election software at this particular moment in November 2020?

A. Based on the first paragraph, it sounds like a lot of counties were getting requests for copies. So I think he -- my guess is he was reiterating to make sure that everybody knew the rules.

Q. Do you recall, in your role as Chief Information Officer, that there was quite a bit of discussion around this time period about people trying to get ahold of copies of election software?

A. Yes.

Q. What do you recall about those discussions?

A. Just that we had moved to a new system. There were people out that had gotten a copy of similar systems of our old and tried to prove that you could breach them, although nobody was ever

actually able to prove that. We have never found anything in the old system, and I think people now that they have a new system, they were just going to try to redo the same exercises of trying to prove that you could breach the new system.

Q. Can you explain what are the reasons that election software is not released to the public? I think you've already touched on this quite a bit in your earlier testimony.

A. It's pretty obvious. You don't expose your -- basically your system to the public because they -- basically you're giving them a road map to how to basically get in and access the system. So the best defense of any system is keeping everything secret about that system.

Q. Has your department ever issued recommendations to physically secure software against unauthorized use or copying?

A. My department, you mean the IT Department?

Q. Yes.

A. We have had conversations with both our counsel and the Elections Department in general of how to communicate different types of security measures to the county. Often Chris Harvey would come to us and say "Hey, I have got to talk to the

counties about this issue, it could be a security issue' or something like that and ask how to phrase it to make sure that it complies with, you know, best practices. Things like that.

Is that what you are asking?

Q. That's among them, yes. And do you recall any such conversations shortly after the 2020 election?

A. I don't recall anything. It doesn't mean it didn't happen because Chris sent messages out to the counties all the time, and he would come consult with me on occasion to help word his messages.

So he may have. I don't keep track or records of them. It was just -- they were conversations.

Q. Did they have any particular urgency, those conversations, in the aftermath of the 2020 election?

A. I don't have any record of that.

Q. Are there protocols in place at the Secretary of State if there is a suspicion that there's been an unauthorized access of election software?

A. We have an Incident Response Plan that we walk through, basically if something comes up that we will walk through to collect information to determine

whether we had an event.

Q. Can you describe briefly for us the steps of that Incident Response Plan?

A. Essentially, first, is to go collect -- you know, collect information initially of what the event was. So, for example, the Fulton County laptop issue, it was -- it was an event. It then turned out it was not an incident. They are different.

So the first thing to do is you collect information from that source. Often we will go directly to, like, Investigations to help us do the research. We will notify the department head, like, that would have been Chris Harvey. We'd have notified Gabe Sterling of it and Ryan Germany, so the key leadership structure, that this is going on.

And then we would start our investigation. In some situations when it seems that we need more high-end forensics, we will bring in an outside source. So we have a company called Fortalice that helps us do forensics work if it's specifically that type of work. And we will go through and collect that.

Oftentimes we will reach out to -- we have contacts at both Homeland Security and FBI and GBI, for Georgia Bureau of Investigation, and we will work

with -- so we have direct contacts to them. They are used to us contacting them on events like this and they go through their process for helping us research it to determine whether this is -- this is really something, an issue or just more of a scare.

Q. You mentioned that there is a distinction between an incident and an event. What's that distinction?

A. Well, when somebody first declares "Oh, this is a problem," we don't call it an incident. It's an event. So we have to basically find out is it real? Is it something -- because once it gets to an incident, then you've got to figure out and start establishing a recovery plan and damage control. But we don't jump into all of those things until we actually can prove that this was real.

So it's -- we have lots of events. Incidents rarely, if ever, happen.

Q. So is it fair to say, then, that something being elevated from an event to an incident is a matter of how much proof there is that you find when you look at it initially?

A. That's essentially how you transition. Someone could say that, that they hacked the system. Okay. So we have this -- we all go do an

imaged or exported, it's just simply that you don't know whether that's true or not; is that fair?

A. That's fair.

MR. DENTON: Object to form.

MR. HAVIAN: Can we go off the record for a bit? I just want to gather my final thoughts and then I will wrap up. So can we just take a five-minute break?

THE VIDEOGRAPHER: The time is 12:59. We are off the record.

(WHEREUPON, a recess was taken.).

THE VIDEOGRAPHER: The time is 1:04. We are back on the record.

Q. (By Mr. Havian) Mr. Beaver, just one last area.

If someone were to obtain an image of the election software, can you give some examples of some of the bad things that someone who had malintent could do with that?

MR. DENTON: Object to form.

A. It will be speculation only. But if somebody has a copy of software, you could essentially go through and get a better understanding of how it works, and basically practice defeating its security. Because no software is someone can walk up

to it without any prior knowledge to it and just defeat it.

So you would have to have -- if you want to defeat a piece of software, you are going to have to have a copy of it. It's kind of like an operating system. To defeat the security in an operating system, you will have to practice defeating it and coming at -- and using the words I used before, "different vectors" to see which ones could actually do it.

So that if somebody had a copy, then they would give them the ability to go find the different vectors to come at it to defeat it.

Q. (By Mr. Havian) And if someone were able to defeat the software security, can you explain what the -- kind of a worst case scenario would be of someone gaining access?

A. So -- and could you tell me which piece of equipment you are talking about?

Q. Election machinery.

A. Okay. And that's a broad spectrum.

MR. DENTON: Object to form.

A. So election machinery includes lots of pieces and parts. Are you talking about the ballot marking device, the scanner --

C E R T I F I C A T E

STATE OF GEORGIA)
) ss.:
FULTON COUNTY)

I, Robin Ferrill, Certified Court Reporter within the State of Georgia, do hereby certify:

That MERRITT BEAVER, VOLUME II, the witness whose deposition is hereinbefore set forth, was duly sworn by me and that such deposition is a true record of the testimony given by such witness.

I further certify that I am not related to any of the parties to this action by blood or marriage; and that I am in no way interested in the outcome of this matter.

IN WITNESS WHEREOF, I have hereunto set my hand this 25th day of March, 2022.

_____

ROBIN K. FERRILL, RPR